# Exhibit B

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF MONROE

| | |
|---|---|
| RAYMOND A. MCLEOD and JUANITA MCLEOD, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>EXCELLUS HEALTH PLAN, INC. and LIFETIME HEALTHCARE, INC.,<br><br>Defendants. | Case No.<br><br>**SUMMONS** |



TO THE ABOVE NAMED DEFENDANTS:

YOU ARE HEREBY SUMMONED and required to serve upon Plaintiffs' attorneys an answer to the Complaint in this action within twenty (20) days after the service of this Summons, exclusive of the day of service, or within thirty (30) days after the service is complete if this Summons is not personally delivered to you within the State of New York. In case of your failure to answer, judgment will be taken against you by default for the relief demanded in the Complaint.

The basis of venue designated is CPLR Section 509, the Defendants' addresses:

Excellus Health Plan, Inc.
165 Court Street
Rochester, New York 14647

Lifetime Healthcare, Inc.
165 Court Street
Rochester, New York 14647

Dated: Rochester, New York
October 19, 2015

Matthew J. Fusco
New York Bar No. 2097046
**TREVETT CRISTO**
**SALZER & ANDOLINA, P.C.**
2 State Street, Suite 1000
Rochester, NY 14614
Telephone: (585) 454-2181
Email: mfusco@trevettcristo.com

**KESSLER TOPAZ**
**MELTZER & CHECK, LLP**
Joseph H. Meltzer
New York Bar No. 5065974
Email: jmeltzer@ktmc.com

Naumon A. Amjed (to be admitted *pro hac vice*)
Email: namjed@ktmc.com

Melissa L. Troutner
New York Bar No. 4178208
Email: mtroutner@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

*Attorneys for Plaintiffs Raymond A. McLeod, Juanita McLeod, and the proposed Class*

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF MONROE

| | |
|---|---|
| RAYMOND A. MCLEOD and JUANITA MCLEOD, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>EXCELLUS HEALTH PLAN, INC. and LIFETIME HEALTHCARE, INC.,<br><br>Defendants. | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

15/1167

FILED
2015 OCT 20 AM 9:13
MONROE COUNTY CLERK

## CLASS ACTION COMPLAINT

Plaintiffs Raymond A. McLeod and Juanita McLeod, individually and on behalf of all others similarly situated, allege the following against Excellus Health Plan, Inc. ("Excellus") and its parent company Lifetime Healthcare, Inc. ("Lifetime") (collectively, "Defendants"), based upon information and belief[1] except as to the allegations pertaining specifically as to Plaintiffs that are based on personal knowledge:

## INTRODUCTION

1. Plaintiffs bring this class action lawsuit individually and on behalf of the putative class against Defendants for their failure to protect Plaintiffs' and putative class members' personally identifiable information and personal health information—including their full names, addresses, birthdates, social security numbers ("SSNs"), telephone numbers, member identification numbers, credit card and financial account information, medical claims

[1] Plaintiffs' information and belief are based on an investigation (by and through counsel) which included, among other things, a review and analysis of publicly available information, news articles, and additional analysis. Plaintiffs believe that substantial additional evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

information, and/or information on Plaintiffs' and putative class members' past, present, or future physical or mental health or condition (collectively, "Sensitive Information"). Plaintiffs and putative class members are current and former members and beneficiaries of Defendants' healthcare insurance plans and other individuals whose Sensitive Information was compromised by Defendants (the "Affected Individuals").

2. Defendants are healthcare insurance providers that finance and deliver healthcare services and are required to protect their customers' Sensitive Information by adopting and implementing the specific data security regulations and standards set forth under the Health Insurance Portability and Accountability Act ("HIPAA"), common law, and New York State law. *See* 45 C.F.R. § 160.103. Defendants expressly and impliedly promised to provide HIPAA protections to their customers—including in Defendants' customer agreements and privacy policies and on Defendants' websites—in exchange for their customers' payments of premiums and/or monies for healthcare services.

3. The Affected Individuals were required to submit their Sensitive Information to Defendants in order to receive healthcare insurance, coverage and/or services or to access Defendants' network. Defendants operate one of the largest healthcare insurance networks in New York State—insuring almost two million individuals and providing healthcare services in thirty one counties in upstate New York. Thus, Defendants are entrusted to protect the private Sensitive Information of millions of individuals and have a duty to take all reasonable measures to protect the Sensitive Information and safeguard it from being compromised.

4. In 2014 and 2015, the healthcare industry, along with other businesses, experienced numerous data breaches that made national headlines. In those same years, government agencies and cybersecurity experts released warnings of persistent threats targeting

the sensitive data that the healthcare industry maintains regarding its customers.[2] Cybersecurity experts also made recommendations about and warned of the lack of technological progress in the healthcare industry regarding cybersecurity.[3]

5. As operators of a large healthcare insurance and healthcare service network that maintained the Sensitive Information of millions of individuals, Defendants were prime targets for hackers. The numerous nationally publicized data breaches, government agency, and cybersecurity expert warnings put Defendants on notice that they were the likely targets of hackers. In fact, the numerous data breaches spurred Defendants to conduct a security assessment of their Information Technology ("IT") systems, which eventually discovered the breach described herein. Defendants' security assessment, however, occurred almost a year after the first nationally publicized data breach of a healthcare company and many months after Defendants had already been hacked.

6. Defendants breached their common law and statutory duties, and contractual promise to protect Plaintiffs' and putative class members' Sensitive Information by allowing hackers to infiltrate Defendants' IT systems and gain access to Plaintiffs' and putative class members' Sensitive Information for approximately twenty months, beginning on or around December 23, 2013. On September 9, 2015, Defendants announced that approximately one month earlier they had discovered hackers had executed an ongoing attack on Defendants' IT systems. The cybersecurity breach—which began on December 23, 2013—allowed the hackers unfettered access to Plaintiffs' and putative class members' Sensitive Information until its discovery on August 5, 2015 (the "Excellus Breach"). Defendants' spokesman Kevin P. Kane

[2] *See infra* Section III:B for a discussion of government and cybersecurity experts' warnings.

[3] *See infra* Section III:B for a discussion of the recommendations of cybersecurity technology experts.

revealed that as many as 10.5 million individuals had their Sensitive Information compromised in the twenty-month Excellus Breach.

7. Moreover, Defendants have failed to notify the Affected Individuals of the scope of and risks associated with the Excellus Breach in an adequate or timely manner. While certain individuals have been notified, Defendants estimate that all Affected Individuals will be notified by November 9, 2015.[4] HIPPA requires that all Affected Individuals be notified without unreasonable delay and no later than 60 days after discovery of the breach of unsecured protected health information. *See* 45 C.F.R. § 164.404.

8. As a result of Defendants' breaches of their common law, statutory, and contractual duties, Plaintiffs and putative class members have suffered and will continue to suffer actual damages and pecuniary losses, including, *inter alia*, costs associated with monitoring and mitigating the risk of identity theft, such as costs for effective credit monitoring services and identity theft insurance, and fees and other costs associated with re-issuing credentials. Given that the type of Sensitive Information compromised can be used to commit fraud years after it was obtained in the Excellus Breach, Defendants' breaches will continue to cause injury to Plaintiffs and Class members in perpetuity. Had Plaintiffs and putative class members known of Defendants' inadequate cybersecurity measures, they would not have purchased Defendants' healthcare coverage or services, and would not have provided Defendants with their Sensitive Information.

9. Plaintiffs request damages to compensate them and putative Class members for current and future losses, and injunctive relief to provide lifetime credit monitoring services and

[4] *See* Home, *A Message from President and CEO, Christopher C. Booth*, EXCELLUS, http://www.excellusfacts.com (last visited Oct. 14, 2015) (hereinafter "Excellus Facts").

identity theft insurance to protect Plaintiffs and the Class members from fraud or identity theft, and after-the-fact identity repair services.

## PARTIES

10. Plaintiff Raymond A. McLeod resides in Seneca Falls, New York, and is a citizen of the State of New York. Mr. McLeod has been enrolled in the Excellus BlueCross BlueShield ("Excellus BCBS") healthcare insurance plan through his union's health and hospital fund since at least March 1, 2013. As a member of Excellus BCBS, Plaintiff entrusted Defendants with his personally identifiable information and personal health information including, *inter alia*, his: SSN, name, address, work address, telephone numbers, and medical history. On September 9, 2015, Mr. McLeod received a letter from Excellus BCBS informing him that Excellus BCBS was the target of a cyber-attack and that "some of [his] personal information may have been accessed by the attackers." *See* Exhibit 1. The letter informed Mr. McLeod that Excellus BCBS would provide two years of free credit monitoring and identity theft protection services. *See id.* The letter also recommended that Plaintiff regularly take additional steps, on his own time, to protect himself from identity theft and fraud. *See id.* Among other things, Defendants recommended that Mr. McLeod expend his own time and resources (1) regularly reviewing the Explanation of Benefits ("EOB") statements Excellus BCBS provides Plaintiff; (2) regularly reviewing bank, credit card, and other financial statements for any unauthorized activity; and (3) placing an alert on or changing Plaintiff's bank account. To date, Mr. McLeod already has expended resources applying for credit monitoring in an attempt to monitor and mitigate the harmful effects of the Excellus Breach. Given the highly sensitive nature of the information compromised by Defendants, Mr. McLeod will be required to continue expending resources for the foreseeable future to monitor and mitigate the harmful effects of the Excellus Breach.

11. Plaintiff Juanita McLeod resides in Seneca Falls, New York, and is a citizen of the State of New York. Mrs. McLeod has been enrolled in the BCBS healthcare insurance plan as a beneficiary of her husband, Plaintiff Raymond A. McLeod, since at least March 1, 2013. As a member of Excellus BCBS, Mrs. McLeod entrusted Defendants with her personally identifiable information and personal health information including, *inter alia*, her: SSN, name, address, work address, telephone numbers, and medical history. Defendants have admitted that beneficiaries like Mrs. McLeod were also impacted by the Excellus Breach. To date, Mrs. McLeod has already expended time applying for credit monitoring and monitoring her credit report in an attempt to monitor and mitigate the harmful effects of the Excellus Breach. Given the highly sensitive nature of the information compromised by Defendants, Mrs. McLeod will be required to continue expending resources for the foreseeable future to monitor and mitigate the harmful effects of the Excellus Breach.

12. Defendant Excellus is a not-for-profit healthcare insurance provider organized under New York State Insurance Law with its headquarters at 165 Court Street, Rochester, Monroe County, New York 14647-0001. Excellus is a licensee of the Blue Cross Blue Shield Association and operates in upstate New York under the following trade names: Excellus BlueCross BlueShield; Excellus BlueCross BlueShield Rochester Region; Excellus BlueCross BlueShield Central New York Region; Excellus BlueCross BlueShield Central New York Southern Tier Region; Excellus BlueCross BlueShield Utica Region; and Univera Healthcare. Excellus conducts extensive business throughout upstate New York and maintains regional headquarters in Buffalo, Rochester, Utica, Elmira and Syracuse and field offices in Watertown, Binghamton, Oneonta, and Plattsburgh. Excellus also contracts with the Federal Government,

thus Excellus's healthcare plans qualify as health maintenance organization ("HMO") plans and preferred provider organization ("PPO") plans for individuals receiving Medicare.

13. Defendant Lifetime is a corporation organized under the laws of New York with its headquarters at 165 Court Street, Rochester, Monroe County, New York 14647-0001. Lifetime is the parent of a number of companies that finance and deliver health care services in upstate New York—all recognized under the trade name The Lifetime Healthcare Companies: Excellus BCBS; Univera Healthcare; Lifetime Benefit Solutions, Inc.; Lifetime Care; Lifetime Health Medical Group; and MedAmerica Insurance Company. As the sole member of Excellus, Lifetime exercises complete control over Excellus such that there is no essential difference between the two entities with respect to, *inter alia*, their headquarters, officers and directors, and the Excellus Breach.

## JURISDICTION AND VENUE

14. This Court has jurisdiction over this matter pursuant to NY CPLR §§ 301 and 302 because Defendants reside in the State of New York and a substantial part of the events or omissions giving rise to the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated from this County.

15. This Court has personal jurisdiction over Excellus because Excellus maintains its principal place of business and resides in Rochester, New York, is incorporated in the State of New York, regularly conducts business in the State of New York, and much of the relevant conduct occurred in the State of New York.

16. This Court has personal jurisdiction over Lifetime because Lifetime maintains its principal place of business and resides in Rochester, New York, is incorporated in the State of New York, regularly conducts business in the State of New York, and much of the relevant conduct occurred in the State of New York.

17. Venue is proper in this Court pursuant to NY CPLR § 503 because both of the Defendants are registered to conduct business in this County, maintain their principal places of business in this County, and reside within this County. Venue is also proper under NY CPLR § 509.

## FACTUAL ALLEGATIONS

### A. The Affected Individuals Trusted Defendants with their Sensitive Information

18. Defendants operate an extensive healthcare insurance and healthcare services network in upstate New York that provides health coverage and health care services to more than 1.6 million people (the "Network").[5] Individuals from across the nation have access to and have accessed Defendants' Network. The actual size of Defendants' Network is demonstrated by the number of individuals whose Sensitive Information was compromised—approximately 10 million as admitted by Defendants on September 9, 2015.[6]

19. In order to obtain healthcare insurance and/or healthcare services from Defendants and/or to access Defendants' Network, the Affected Individuals were required to submit the following highly sensitive personal information: names, member identification numbers, SSNs, addresses, type of healthcare benefits, payment amounts, and payment information.

20. Because Defendants' Network contains healthcare insurance and healthcare services, Defendants provide all individuals who access Defendants' Network with their Privacy Notice. *See* Exhibit 2. In the Privacy Notice, Defendants promise to safeguard health

[5] *See* Home, About Us, THE LIFETIME HEALTHCARE COMPANIES, http://www.lifethc.com/about.html (last visited Oct. 14, 2015).

[6] *See* Andy Greenberg, *Hack Brief: Health Insurer Excellus Says Attackers Breached 10M Records*, WIRED, Sept. 10, 2015, http://www.wired.com/2015/09/hack-brief-health-insurance-firm-excellus-says-attackers-breached-10m-records/.

information and nonpublic personal information provided to them, which together comprise Plaintiffs' and Class members' Sensitive Information. *See id.* at 1-2. Defendants' promise and the information in the Privacy Notice is repeated and expanded throughout all of Defendants' major websites.[7]

21. For example, Defendant Lifetime states in its Privacy Policy that "[w]hether you are a current customer or just visiting our Web Site, we are committed to protecting the personal information you provide just as we are committed to protecting your personal information when you provide it to us over the phone, in person or through the mail."[8]

22. Defendant Excellus in its Privacy Policy states that it is "committed to protecting any personal information that you provide us on this website according to applicable laws, regulations and accreditation standards and practices, and we continue to evaluate new administrative, technical and physical safeguards for protecting your information."[9]

23. Specifically, the Privacy Notice states that Defendants are "required by applicable federal and state laws to maintain the privacy of . . . ." members' Sensitive Information. Furthermore, Defendants expressly recognize that they must follow the privacy practices enumerated in the Privacy Notice including, *inter alia*, (1) conducting reviews of privacy practices by a privacy oversight committee; (2) establishing a security coordinator to detect and prevent security breaches; and (3) maintaining security protections in all computer systems that contain Sensitive Information. *See* Exhibit 2 at 5. Defendants also promise that they will not

---

[7] *See* Privacy, *Our Privacy Policy*, THE LIFETIME HEALTHCARE COMPANIES, http://www.lifethc.com/privacy.html, last visited Oct. 5, 2015 (hereinafter "Lifetime Privacy policy"); Privacy Policy, *Website Privacy Policy*, EXCELLUS BCBS, https://www.excellusbcbs.com/wps/portal/xl/!ut/p/b1/04_SjzQ0MzI0tjA1ttCP0I_KSyzLTE8syczPS8wB8aPM4kNCg0x8zD2MDCyCPNwMPL293V2N_HwMDIwMgAoikRW4ewaYG3iahPkEW5oHGBmYGBKn393LLNjFy9LJzMnE18DMy8UowAAKiNNvgAM44tcfaITufkwF-PSbmRLQD1SAT7-rAQH9rgT97-eRn5uqnxuV4wYCFo6KigCs5Ysy/dl4/d5/L2dJQSEvUUt3QS80SmtFL1o2X1RVUjRMN0gyMDhSSEYwSUtLR0UyTkwwMFU2/ last visited Oct. 5, 2015 (hereinafter "Excellus Website Privacy Policy").

[8] Lifetime Privacy Policy, *supra* note 7.

[9] Excellus Website Privacy Policy, *supra* note 7.

disclose members' Sensitive Information to anyone unless they are permitted to do so by law or have received a signed authorization from the member. *See id.* at 2. Lastly, Defendants promise to notify members of any breach of members' Sensitive Information. *See id.* at 1.

24. In addition to Defendants' stated commitments and common law duties to protect Plaintiffs' and putative class members' Sensitive Information, HIPAA requires healthcare providers like Defendants to adopt administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of consumers' Sensitive Information. The Excellus Breach demonstrates that Defendants failed to honor their express promises and obligations under law. Among other things, Defendants failed to:

- ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and/or transmitted in accordance with 45 C.F.R. § 164.306(a)(1);
- "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information" which would restrict access only to those persons or software programs that have been granted access rights in accordance with 45 C.F.R. § 164.312(a)(1);
- "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations" in accordance with 45 C.F.R. § 164.308(a)(1)(i);
- "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of" electronic protected health information in accordance with 45 C.F.R. § 164.306(a)(2); and
- protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding

individually identifiable health information in accordance with 45 C.F.R. § 164.306(a)(3).

25. Defendants acknowledge the importance their members and customers place on privacy in the statements on Defendants' websites and in their Privacy Notice. Thus, Defendants are and were aware of their duty to safeguard the Affected Individuals' Sensitive Information and to promptly notify Affected Individuals of any compromise of their Sensitive Information, and knew that the Affected Individuals were relying on them to properly perform those duties.

### B. Defendants Were on Notice that the Healthcare Industry is a Major Target of Hackers

26. On April 8, 2014, the Federal Bureau of Investigation's ("FBI") Cyber Division released a Private Industry Notification for healthcare sector companies, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and advised that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise."[10] A few months later, in August 2015, the FBI issued a "Flash" alert warning that healthcare companies are being targeted by hackers. The "Flash" alert warned healthcare companies that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[11]

---

[10] Private Industry Notification, *(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION, Apr. 8, 2014, *available at* http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[11] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS, Aug. 20, 2014, http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

27. The Identity Theft Resource Center ("ITRC"), an organization that focuses on fraud and identity theft education, publishes the ITRC Breach Report annually, which tracks the number of data breaches in a calendar year and records exposed as a result of the breaches that year. The ITRC Breach Report for 2013 noted that the healthcare sector accounted for 44.1%, or 271 out of 614 breaches in 2013—by far the most out of any other sector including, *inter alia*, business and the government. In 2014, the ITRC Breach Report noted that the healthcare sector again topped every other sector and accounted for 42.5%, or 333 out of 783 breaches.

28. The most prominent breach of a healthcare company in 2014 involved Community Health Systems, Inc. ("Community Health"), a publicly traded hospital operator. On August 18, 2014, Community Health announced that the information of 4.5 million patients was stolen in a cyber-attack that may have originated in China. Community Health disclosed that hackers may have obtained patient names, birth dates, addresses, telephone and SSNs.[12]

29. After two major healthcare data breaches were announced in the first quarter of 2015, *The Washington Post* identified 2015 as the year of the healthcare hack.[13] The first major data breach of 2015 was announced by healthcare insurance company Anthem, Inc. ("Anthem").[14] In February 2015, Anthem announced that hackers had compromised the records of 78.8 million individuals, including 60 to 70 million of its current and former customers and employees and millions of members of other healthcare insurance companies. The compromised information included, *inter alia*, names, birthdays and SSNs. One month later, in

---

[12] *See* Nicole Perlroth, *Hack of Community Health Systems Affects 4.5 Million Patients*, THE NEW YORK TIMES, Aug. 18, 2014, http://bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients/?_r=0.

[13] *See* Andrea Peterson, *2015 is already the year of the health-care hack – and – it's only going to get worse*, THE WASHINGTON POST, Mar. 20, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/.

[14] *See* Anna Wilde Mathews, *Anthem: Hacked Database Included 78.8 Million People*, THE WALL STREET JOURNAL, Feb. 24, 2015, http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364.

March 2015, healthcare insurer Premera Blue Cross ("Premera") announced that hackers had compromised the data of 11 million individuals in an attack that began in May 2014.[15] Premera reported that the hackers gained access to, *inter alia*, patient medical information, bank account numbers, SSNs, and birthdates.

30. Cybersecurity experts have recognized that healthcare companies are particularly vulnerable to hackers because the companies do not spend enough money on cybersecurity, rely on legacy systems for data protection, and are slow to adopt technological advances in cybersecurity. After the Anthem Breach, Martin Walter, a senior director at network security company RedSeal, stated "[i]t was only a matter of time until hackers found out that it's much easier to go after Social Security numbers and personally identifiable information with healthcare providers, which in comparison spend significantly less on security, making them tentatively easier targets." As expressed by another cybersecurity expert, healthcare companies are "storing treasure troves of information and are not doing enough to protect it."[16]

31. According to Dave Kennedy, Chief Executive Officer ("CEO") of information security firm TrustedSEC, healthcare organizations are targets because they store data with substantial resale value in black markets and have security practices that are less sophisticated than other industries. In a *Washington Post* article Kennedy noted that "health organizations sometimes rely on legacy systems, and some have not invested in cybersecurity at a rate that matches the urgency of the threats they face."[17] Kennedy states that "[t]he medical industry is

---

[15] *See* Peterson, *supra* note 13.

[16] Tim Greene, *Anthem hack: Personal data stolen sells for 10X price of stolen credit card numbers*, IT WORLD, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[17] Peterson, *supra* note 13.

years behind other industries when it comes to security."[18] In fact, according to cybersecurity firm WhiteHat, only 24% of known security flaws in the healthcare industry are fixed.[19] As another healthcare industry expert observed, "health care has been very slow to adopt almost every technological advance," also adding that "[r]ight now, a lot of health care companies are sitting ducks."[20]

32. Starting as early as 2014, the FBI warnings, numerous data breaches suffered by prominent healthcare insurers and healthcare providers, and analyst recommendations placed Defendants on notice of the legitimate threat posed by hackers and the need for Defendants to provide adequate measures to safeguard the Affected Individuals' Sensitive Information.

**C. The Excellus Breach**

33. On September 9, 2015, Defendants announced that they had discovered a cyber-attack had targeted their IT Systems.[21] Defendants discovered the attack after hiring FireEye's Mandiant ("Mandiant") incident response division to conduct a forensic assessment of their IT systems.[22]

34. On August 5, 2015, Mandiant's forensic assessment revealed that hackers gained unauthorized access to Defendants' IT systems on or about December 23, 2013.[23] The assessment and subsequent investigation of the Excellus Breach revealed that the hackers

---

[18] *Id.*

[19] *See* Jaikumar Vijayan, *Premera hack: What criminals can do with your healthcare data*, THE CHRISTIAN SCIENCE MONITOR, Mar. 20, 2015, http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data.

[20] J.K. Wall, *Anthem's IT system had cracks before hack*, INDIANAPOLIS BUSINESS JOURNAL, Feb. 14, 2015, http://www.ibj.com/articles/51789-anthems-it-system-had-cracks-before-hack.

[21] News Releases, *Excellus BCBS Offers Protection for Affected Individuals Following Cyberattack*, PR NEWSWIRE, Sept. 9, 2015, http://www.prnewswire.com/news-releases/excellus-bcbs-offers-protection-for-affected-individuals-following-cyberattack-300140371.html (hereinafter "Excellus Press Release").

[22] *See id.*

[23] *See* Greenberg, *supra* note 6.

compromised approximately 7 million individuals' information, which included names, date of births, SSNs, mailing addresses, telephone numbers, member identification numbers, financial account information, and medical claims information.[24]

35. Defendants' spokesman, Kevin Kane, later updated the number of potential individuals affected by the Excellus Breach to between 10 and 10.5 million, and reported that the compromised financial payment information included some of the Affected Individuals' credit card numbers.[25] Kane acknowledged that hackers were able to gain administrative access to Defendants' network despite Defendants' encryption of the Sensitive Information, likely by gaining access to decryption keys available to system administrators.[26] As a result of Defendants' inadequate cybersecurity systems, hackers were able to access the Affected Individuals' Sensitive Information through Defendants' IT systems undetected for nearly two years.

36. Indeed, Adam Kujawa, malware intelligence leader at cybersecurity firm Malwarebytes, recently stated "[w]ith an attack of this magnitude, being done over the course of more than a year, cybercriminals probably stole information by simply copying and pasting it from its unencrypted form on the secure network to their own systems, or utilizing built-in tools to parse the information for the most valuable data."[27]

37. Defendants' President and CEO, Christopher C. Booth, has attempted to reassure customers of the steps Defendants are taking to protect Affected Individuals, and Defendants have created a website informing Affected Individuals about the Excellus Breach. On the

---

[24] *See* Excellus Press Release, *supra* note 21.

[25] *See* Greenberg, *supra* note 6.

[26] *See id.*

[27] John P. Mello Jr., *Hackers Home in on Health, Education, Government Sectors*, TECHNEWSWORLD, Sept. 16, 2015, http://www.technewsworld.com/story/82495.html.

website, Booth asserts that "[s]afeguarding the privacy of your personal information is a top priority for us, and we make every effort to protect your information . . . . We are committed to making sure you get the tools and assistance you need to help protect you."[28] The website states that the Excellus Breach "affects members, patients, or others who have done business with the impacted plans," and contains a frequently asked questions ("FAQ") section that provides the same information and recommendations contained in the letter sent to Plaintiff Raymond A. McLeod.[29] However, the steps Defendants have taken to purportedly protect the Affected Individuals from the Excellus Breach—including providing two years of free identity theft protection services through Kroll and credit monitoring from TransUnion—are wholly inadequate and in no way provide sufficient protection for Plaintiffs and Class members from the harm caused by Defendants' unlawful conduct.

38. Moreover, the Affected Individuals include, *inter alia*, the beneficiary minor children of Defendants' customers and minor children who accessed Defendants' Network. Defendants' letters and information on their websites offer conflicting information as to what protections Defendants are providing individuals under 18 years old. Although Defendants' website informs all Affected Individuals that the Defendants are providing two years of free credit monitoring and identity theft consultation and restoration services, the letter sent to the Affected Individuals states that they need to be 18 years or older to receive the services. *See* Exhibit 1. Specifically, Defendants' letter states that "[t]o receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file." *Id.* Thus, Defendants are only providing credit monitoring and identity theft restoration services to

[28] Excellus Facts, *supra* note 4.

[29] *Compare* Exhibit 1 *with* Excellus Facts, *supra* note 4 at FAQ section.

individuals who are 18 years old or older, and there is no protection offered by Defendants for minors affected by the Excellus Breach.

### D. The Ramifications of the Excellus Breach

39. The compromise of the Affected Individuals' Sensitive Information leaves them indefinitely vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and other criminal transgressions. Noted cybersecurity experts have explained that the type of data stolen in the Excellus Breach is particularly sensitive, and can cause heightened injury to Affected Individuals. "When someone has your clinical information, your bank account information, and your Social Security number, they can commit fraud that lasts a long time . . . . Th[is] kind of identity theft . . . . is qualitatively and quantitatively different than what is typically possible when you lose your credit card . . . ."[30]

40. The compromise of Plaintiffs' and Class members' SSNs poses particularly difficult challenges as SSNs can be used to open bank accounts, credit cards and medical accounts, gain employment, secure loans, and obtain medical care, among other things.

41. Tax fraud is one of the major transgressions that identity thieves can commit with compromised SSNs. Over the past years, there has been a significant increase in the incidence of fraudulent tax filings. In 2013, the Internal Revenue Service paid an estimated $5.2 billion in tax refunds obtained from identity theft and that same year it prevented an additional $24.2 billion in fraudulent tax refund transfers.[31] Individuals typically discover they have been the victims of a fraudulent tax return only when an individual's authentic tax return is rejected.

---

[30] Vijayan, *supra* note 19.

[31] *See* Shan Li, *FBI probes rash of fraudulent state tax returns filed through TurboTax*, LOS ANGELES TIMES, Feb. 21, 2015, http://www.latimes.com/business/la-fi-turbotax-fbi-20150212-story.html.

42. Unlike compromised credit cards or bank accounts which can be canceled or changed, compromised SSNs are difficult to change or cancel. To obtain new SSNs, individuals must complete significant paperwork and show evidence of actual SSN misuse. Thus, individuals are not permitted to take preventive action to defend against the possibility of misuse—individuals must show evidence of actual fraudulent activity to obtain a new SSN.

43. Even if individuals obtain new SSNs, there are no guarantees that the new SSN will remain clean of any past fraudulent activities. According to Julie Ferguson of the ITRC, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[32]

44. Minors whose SSNs have been compromised face even greater challenges in protecting themselves from identity theft and fraud. It could be years before minors apply for any type of credit, such as student loans, and discover thieves stole their SSN and tainted their credit history. Parents of children under 13 years old can request a credit report for their children but the process is cumbersome. For example, parents have to physically mail the following information and documentation: the child's legal name, birth date and address; a certified copy of the child's birth certificate; a copy of the child's Social Security card; a copy of the parent's driver's license or government-issued identity card with the parent's current address; and a copy of a current utility bill with the same address.[33]

45. Whereas adults have credit reports that they can periodically monitor, most minors have no credit report to monitor. Having no credit report means that, in most states, a

---

[32] Brian Naylor, *Victims of Social Security Number Theft Find it's Hard To Bounce Back*, NPR, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[33] *See* Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, KIPLINGER, Feb. 10, 2015, http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html#.

minor cannot "freeze" his or her credit account in order to block identity thefts from opening new lines of credit on the account—in order to "freeze" a minor's credit report, a credit report must exist. Credit reporting bureaus may allow a parent to create a credit report for minors for the purpose of freezing it the report. However, as detailed above the process is cumbersome. Defendants have not provided any credit theft or identify protection for minors or detailed any steps parents can take to ensure that minor children whose Sensitive Information has been compromised in the Excellus Breach do not become victims of identity theft and/or fraud.

46. Another danger the Affected Individuals face as a result of the compromise of their Sensitive Information is medical fraud as identity thieves often use stolen SSNs to obtain medical care in someone else's name. The Ponemon Institute concluded in a study of medical fraud victims that victims spend on average $13,500 to resolve problems arising from medical identity theft.

47. Medical identity fraud affected 2.3 million people in 2014—an increase of 21% over the previous year. Medical identity fraud can also have non-financial impacts. For example, Deborah Peel, executive director of Patient Privacy Rights, has described scenarios in which an individual may receive the wrong treatment because another person has compromised the individual's medical records. For example, an individual may be given the wrong type of blood in a blood transfusion or may be proscribed the wrong type of medicines because the individual's medical records contain information supplied by an individual obtaining treatment under a false name. Defendants' proposed remedies offer Plaintiffs and Class members no protection from medical identity fraud.

48. The Sensitive Information compromised in the Excellus Breach is more valuable than the credit card information compromised in other nationally publicized data breaches as

credit card numbers can be canceled or changed to avoid future harm and victims can get fraudulent charges dismissed. As detailed above, some of the Sensitive Information compromised in the Excellus Breach is difficult, if not impossible, to change or cancel.

49. Because the type of data contained in the Excellus Breach provides identity thieves the ability to commit many types of fraud, the data demands a higher price in the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[34]

50. In fact, Mr. Walter's estimate may be low. According to a recent PricewaterhouseCoopers report, an identity theft kit containing health insurance credentials can be worth up to $1,000 on the black market, while stolen credit cards may go for $1 each. Further, a report released by the Ponemon Institute in late February concluded that 65% of medical identity theft victims pay more than $13,500 out of pocket to resolve identity theft issues and spend 200 hours with insurers and providers to secure their credentials, and check the accuracy of their personal information, invoices, and e-health records.[35]

51. The aforementioned information highlights the serious risk that the Excellus Breach has imposed on the Affected Individuals. Defendants' remedies in response to the Excellus Breach do very little to actually prevent fraud. As noted cybersecurity blogger Brian Krebs has explained "the sad truth is that most [credit monitoring] services offer little in the way of real preventative protection against the fastest-growing crime in America [identity theft]."[36]

---

[34] Greene, *supra* note 16.

[35] *See* Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, PONEMON INSTITUTE, Feb. 2015, *available at* http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/.

[36] Brian Krebs, *Are Credit Monitoring Services Worth It?*, KREBS ON SECURITY, Mar. 14, 2014, http://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/.

Furthermore, the credit monitoring services offered by Defendants only cover one credit report—the report by the credit agency TransUnion. Although Defendants offer free identity theft restoration services, the damage will already be done to Plaintiffs and Class members by the time they need restoration services.

52. As a result of Defendants' conduct, the Affected Individuals have suffered and will continue to suffer extensive harm, injury, and damages.

**PLAINTIFFS' AND CLASS MEMBERS' DAMAGES**

53. Plaintiffs and millions of Class members have been seriously harmed by Defendants' uniform mishandling of their Sensitive Information. Highly sensitive and personal information about Plaintiffs' and Class members' has been stolen and is now in the hands of criminals to be bought, sold, or otherwise distributed for the purpose of misappropriating Plaintiffs' and Class members' identities or property. Only through aggressive and comprehensive identity theft solutions can the security of Plaintiffs' and Class members' identity be maintained in the wake of the Excellus Breach, if at all.

54. Plaintiffs and Class members have suffered and will continue to suffer damages, including actual damages, pecuniary losses and lost time and resources expended responding to the Excellus Breach caused by Defendants. Plaintiffs and Class members have already suffered, will continue to suffer, and/or have an increased risk of suffering from:

- out-of-pocket costs associated with the monitoring, prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts;
- current and future costs in terms of time, effort, and money that will be expended to monitor, prevent, detect, contest, and repair the impact of the Sensitive

Information compromised as a result of the Excellus Breach for the remainder of Plaintiffs' and Class members' lives;

- the loss of opportunity to control how their Sensitive Information is used;
- the diminution in the value and/or use of their Sensitive Information entrusted to the Defendants for the purpose of receiving healthcare insurance and healthcare services from the Defendants;
- the compromise, publication, and/or theft of their Sensitive Information;
- lost opportunity costs associated with effort expended and the loss of productivity from monitoring, addressing and/or attempting to mitigate the actual and future consequences of the Excellus Breach, including, *inter alia*, efforts spent researching how to prevent, monitor, detect, contest, and recover from identity and health care/medical data misuse;
- costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports, and assets;
- unauthorized use of compromised Sensitive Information to open new financial and/or health care or medical accounts; and
- the continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information in their possession.

55. Defendants' proffered remedies are woefully inadequate to protect against or compensate the Affected Individuals for the above risks.

56. First, the particular credit monitoring services being offered to victims do not provide comprehensive protection. While the services offer a limited version of traditional credit monitoring, they do not offer the more robust features of a premium three-bureau, modern identity service, which is necessary in this instance due to the breadth of the information compromised in the Excellus Breach.

57. However, even traditional credit monitoring at its best is only effective for a relatively small portion of the identity and reputational crimes these particular victims can be subjected to, due to the Sensitive Information compromised in the Excellus Breach. A report by all three major credit reporting agencies will generally catch new credit account fraud in traditional areas. But criminals can still actively sell the victims' data to underworld sites for tax identity theft, medical identity theft, and other difficult to detect forms of identity crime such as synthetic identity theft, identity theft of medical information or insurance information, or theft of professional credentials. Thieves also frequently target breach victims with malware, phishing attacks, and "key-logger" attacks. Thieves frequently use mobile payment and social media sites and newer forms of credit payment like Amazon and EBay for committing fraud. Any credit monitoring service offered to victims of this extensive breach needs to offer added protection, including software and other technical support to detect malware and other malicious attacks targeting Affected Individuals. For all these reasons, credit monitoring alone is insufficient to repair the damage done by the Excellus Breach.

58. Second, the proposed remedies do not appear to include comprehensive monitoring for criminal data sales on the dark web sites and data broker sites that deal in stolen data. This comprehensive monitoring is a necessary service that is offered for victims of

identity theft and data breaches, particularly where the data stolen is as sensitive as it was in the Excellus Breach.

59. Third, the two year duration of credit monitoring services Defendants offer are far too short. It is well-documented by law enforcement professionals and identity theft experts that hackers "season" data by allowing it to age for a few years.[37] The more sensitive and potentially valuable the data is, the more it can be seasoned by criminals. The Sensitive Information compromised in the Excellus Breach, which includes SSNs, financial account information, and medical information, warrants lifetime protection due to the completeness of the data and its high value on the black market. Finally, as discussed above, no protection has been offered for minors affected by the Excellus Breach.

60. Plaintiffs and Class members have and will continue to reasonably incur expenses to avoid or mitigate the harm caused by the Excellus Breach. Thus, Plaintiffs and Class members already have suffered damages as a result of Defendants' conduct and will continue to suffer damages throughout their lifetimes. The nature of the Sensitive Information compromised in the Excellus Breach is so confidential and sensitive that it can be used to replicate identities and inflict harm on Plaintiffs and Class members in perpetuity. Accordingly, there is an ongoing substantial risk of harm to the Affected Individuals that requires Plaintiffs and Class members to monitor, among other things, their financial accounts and credit reports for life. This significant expenditure of time and resources by Plaintiff and Class members to protect themselves from identify theft and other harms is a result of Defendants' conduct and the Excellus Breach, and would not have occurred but for Defendants' conduct.

---

[37] Lilian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets For Cybercrime Tools and Stolen Data: Hackers' Bazaar*, RAND, 35, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf (last visited Oct. 14, 2015).

## CLASS ALLEGATIONS

61. Plaintiffs bring this action individually and on behalf of all others similarly situated, and ask the Court to certify the class defined below as a class action pursuant to New York statute CPLR § 901.

62. Plaintiffs bring this action on behalf of the following Class: All persons in the United States whose Sensitive Information was compromised as a result of the Excellus Breach announced on September 9, 2015 (the "Class").

63. Excluded from the proposed Class are Excellus and Lifetime, as well as their agents, officers, directors, and their families as well as Excellus's and Lifetime's parents, subsidiaries, and corporate affiliates. Any judicial officer assigned to this case, is also excluded. Plaintiffs reserve the right to revise the definition of the Class based upon subsequently discovered information.

64. The Class is so numerous that joinder of all members is impracticable. Plaintiffs believe that there are at least millions of proposed Class members throughout the United States.

65. Common questions of law and fact exist as to all members of the Class and predominate over any issues solely affecting individual members of the Class. The common questions of law and fact include but are not limited to:

a. whether Defendants owed a duty to Plaintiffs and Class members to take reasonable measures to protect and safeguard Plaintiffs' and Class members' Sensitive Information;

b. whether Defendants breached their duties to secure Plaintiffs' and Class members' Sensitive Information;

c. whether Defendants' breach of their duties caused the Excellus Breach and/or the compromise of Plaintiffs' and Class members' Sensitive Information;

d. whether Defendants knew or should have known that their cybersecurity systems were vulnerable to attack;

e. whether an express or implied contract existed between Defendants and Plaintiffs and Class members;

f. whether Defendants breached their express or implied contracts with Plaintiffs and Class members;

g. whether Defendants' failure to employ adequate cybersecurity practices to protect Plaintiffs' and Class members' Sensitive Information was a deceptive act or unfair trade practice in violation of New York General Business Law § 349(a);

h. whether Defendants' benefited from retaining Plaintiffs' and Class members' payments for services but not providing adequate cybersecurity services to protect Plaintiffs' and Class members' sensitive information;

i. whether Plaintiffs and Class members were harmed by Defendants' breaches and/or unlawful conduct; and

j. whether Plaintiffs and Class members are entitled to recover actual damages and/or punitive damages.

66. Plaintiffs' claims are typical of the claims of the Class. As alleged herein, Plaintiffs and the Class all sustained damages arising out of the same course of unlawful conduct by Defendants.

67. Plaintiffs are willing and prepared to serve the Class in a representative capacity with all of the obligations and duties material thereto. Plaintiffs will fairly and adequately protect the interests of the Class and have no interests adverse to, or which conflict with, the interests of other members of the Class.

68. Plaintiffs' interests are co-extensive with, and not antagonistic to, those of the absent Class members. Plaintiffs will undertake to represent and protect the interests of the absent Class members.

69. Plaintiffs have engaged the services of the undersigned counsel. Counsel is experienced in complex litigation, including class action litigation involving data breaches, will adequately prosecute this action, and will assert and protect the rights of, and otherwise represent, Plaintiffs and the absent Class members.

70. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiffs know of no difficulty to be encountered in the management of this litigation that would preclude its maintenance as a class action.

71. The interest of Class members in individually controlling the prosecution of separate actions is theoretical and not practical. The Class has a high degree of similarity and is cohesive. Plaintiffs anticipate no difficulty in the management of this matter as a class action.

## CLAIMS

### FIRST CLAIM
### Breach of Contract
### On behalf of Plaintiffs and the Class

72. Plaintiffs incorporate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

73. Plaintiffs and Class members paid money to Defendants in exchange for healthcare coverage and/or services, which included Defendants' promises to secure, safeguard, protect, keep private and not disclose Plaintiffs' and Class members' Sensitive Information.

74. In documents that memorialize the obligations of the contracting parties, Defendants promised Plaintiffs and Class members that Defendants would protect, secure, keep private, and not disclose Plaintiffs' and Class members' Sensitive Information. Defendants

further promised to safeguard Plaintiffs' and Class members' Sensitive Information from being accessed, copied, and transferred by or disclosed to third parties. Defendants were further obligated to provide Plaintiffs and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of Plaintiffs' and Class members' Sensitive Information.

75. These documents were provided in a manner and during a time where they became part of the agreements of services, and were express contracts between Defendants and the Affected Individuals.

76. As part of their express agreements, Defendants promised to comply with all HIPAA standards and to make sure that Plaintiffs' Sensitive Information was protected, secured, kept private, and not disclosed.

77. In the alternative, to the extent it was not expressed, an implied contract existed whereby, Defendants promised to comply with all HIPAA standards and regulations and to ensure that Plaintiffs' and Class members' Sensitive Information was secured, safeguarded, kept private, protected, and not disclosed to third parties.

78. To the extent it was not expressed, an implied contract was created whereby Defendants promised to safeguard Plaintiffs' and Class members' Sensitive Information from being accessed, copied, and transferred by or disclosed to third parties.

79. To the extent it was not expressed, an implied contract existed between the parties whereby, in exchange for payment from Plaintiffs and Class members, Defendants agreed to protect, safeguard, secure, keep private, and not disclose to unauthorized third-parties Plaintiffs' and Class members' Sensitive Information. Under the implied contract, Defendants were further obligated to provide Plaintiffs and Class members with prompt and sufficient notice of

any and all unauthorized access and/or theft of Plaintiffs' and Class members' Sensitive Information.

80. Defendants did not secure, safeguard, protect, and/or keep private Plaintiffs' and Class members' Sensitive Information and/or disclosed Plaintiffs' and Class members' Sensitive Information to unauthorized third parties. Thus, Defendants breached their contracts with Plaintiffs and Class members.

81. Defendants further breached their contracts with Plaintiffs and Class members by allowing unauthorized third parties to access, copy, and transfer Plaintiffs' and Class members' Sensitive Information.

82. Defendants further breached their contracts with Plaintiffs and Class members by failing to provide prompt and sufficient notice of any and all unauthorized access and/or theft of Plaintiffs' and Class members' Sensitive Information.

83. Defendants' failure to satisfy their confidentiality and privacy obligations resulted in Defendants providing services to Plaintiffs and Class members that were of a diminished value and resulted in the compromise of Plaintiffs' and Class members' Sensitive Information and the burden of monitoring and repairing Plaintiffs' and Class members' credit reports going forward.

84. As a result of Defendants' breaches, Plaintiffs and Class members have been and will continue to be harmed, damaged, and/or injured.

85. Plaintiffs and Class members seek actual damages as described herein to be proven at trial, and attorneys' fees and costs as permitted by law.

**SECOND CLAIM**
**Negligence**
**On behalf of Plaintiffs and the Class**

86. Plaintiffs incorporate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

87. Defendants had a duty to exercise reasonable care to protect and secure Plaintiffs' and Class members' Sensitive Information in their possession or control from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

88. This highly confidential Sensitive Information includes but is not limited to full legal names, birth dates, SSNs, medical identification numbers, health histories, street addresses, email addresses, employment information, income data, and other personal information.

89. Defendants' duties included, among other things, designing, maintaining, and testing their cybersecurity systems to ensure that Plaintiffs' and Class members' Sensitive Information in Defendants' possession or control was adequately secured and protected, was retained only for legitimate purposes and with adequate storage, retention, security, and disposal policies, and was not disclosed to unauthorized parties.

90. Moreover, Defendants had a duty to implement processes that would detect a breach in their cybersecurity systems in a timely manner, and to notify the Affected Individuals of the Excellus Breach in a timely manner and without unreasonable delay.

91. Defendants' duties arise from the common law, as well as principles embodied in New York statutory law, and HIPAA.

92. In light of the special relationship between Plaintiffs and Class members and Defendants, whereby Defendants required Plaintiff and Class members to provide highly sensitive confidential Sensitive Information as a condition of application, availability of health

insurance or healthcare services, and claims reimbursement, Defendants undertook a duty of care to ensure the security of such information.

93. Defendants also knew or should have known that hackers would target Plaintiffs' and Class members' highly confidential Sensitive Information. Indeed, countless data breaches in the past year have exploited similarly lax security controls to gain access to company-wide databases. Moreover, a number of these data breaches have targeted medical companies or institutions and the Sensitive Information of their members. As a result, it was known to Defendants, or at least reasonably foreseeable, that Plaintiffs' and Class members' Sensitive Information was a high value target to hackers. Thus, Defendants had a duty to take reasonable steps to protect and safeguard Plaintiffs' and Class members' Sensitive Information.

94. Through their acts or omissions, Defendants breached their duty to use reasonable care to protect and safeguard Plaintiffs' and Class members' Sensitive Information in Defendants' possession or control. Defendants breached their duty by (1) failing to adopt, implement, and maintain adequate cybersecurity measures to safeguard Plaintiffs' and Class members' Sensitive Information; (2) failing to adequately monitor the security of Defendants' Network; (3) allowing unauthorized access to Plaintiffs' and Class members' Sensitive Information; (4) failing to recognize in a timely manner that Plaintiffs' and Class members' Sensitive Information had been compromised; and (5) failing to notify Plaintiffs and Class members in a timely manner that their Sensitive Information had been compromised. Indeed, Defendants' negligent cybersecurity systems failed to detect the breach for 20 months, giving hackers ample time to bypass any encryption Defendants used to protect Plaintiffs' and Class members' Sensitive Information.

95. Defendants' failure to comply with industry standards relating to cybersecurity further evidences Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Sensitive Information in Defendants' possession or control.

96. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiffs and Class members, the Excellus Breach would not have occurred and Plaintiffs' and Class members' Sensitive Information would not have been compromised.

97. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable and probable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Sensitive Information in Defendants' possession or control. Defendants knew or should have known that their systems and technologies for processing and securing Plaintiffs' and Class members' Sensitive Information had significant vulnerabilities and were subject to breach.

98. As a result of Defendants' negligence, Plaintiffs and Class members have suffered damages that have included or may include without limitation (l) the loss of the opportunity to control how their Sensitive Information is used; (2) the diminution in the value and/or use of their Sensitive Information entrusted to Defendants for the purpose of obtaining healthcare coverage or services with the understanding that the Defendants would safeguard their Sensitive Information against theft and not allow access to and misuse of their Sensitive Information by others; (3) the compromise, publication, and/or theft of their Sensitive Information; (4) out-of-pocket costs associated with the prevention, monitoring, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to

mitigate the actual and future consequences of the Excellus Breach, including but not limited to efforts spent researching how to prevent, monitor, detect, contest, and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised Sensitive Information to open new financial and/or health care or medical accounts and/or medical treatment; (8) the continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further breaches as long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information; and (9) future costs in terms of time, effort, and money that will be expended to monitor, prevent, detect, contest, and/or repair the impact of the Sensitive Information compromised as a result of the Excellus Breach for the remainder of Plaintiffs' and Class members' lives.

**THIRD CLAIM**
**Restitution/Unjust Enrichment**
**(In the alternative to Breach of Contract)**
**On behalf of Plaintiffs and the Class**

99. Plaintiffs incorporate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

100. If the Court finds Plaintiffs' and Class members' contracts with Defendants to be invalid, non-existent, or otherwise unenforceable, Plaintiffs and Class members may be left without any adequate remedy at law.

101. Defendants received payment from Plaintiffs and Class members to perform services that included adequately protecting and safeguarding Plaintiffs' and Class members' Sensitive Information.

102. Defendants did not protect Plaintiffs' and Class members' Sensitive Information, but retained Plaintiffs' and Class members' payments. Thus, Defendants benefitted from receiving Plaintiffs' and Class members' payments without incurring the expense of adequately protecting and safeguarding Plaintiffs' and Class members' Sensitive Information from unauthorized disclosure.

103. Defendants retained the benefits of Plaintiffs' and Class members' payments under circumstances which render it inequitable and unjust for Defendants to retain such benefits without paying for their value.

104. Defendants have knowledge of said benefits.

105. Accordingly, under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members, because Defendants failed to implement (or adequately implement) the data management and cybersecurity measures that Plaintiffs and Class members paid for and that were otherwise mandated by HIPAA regulations, federal and state laws, and industry standards.

**FOURTH CLAIM**
**Violation of N.Y. Gen. Bus. Law § 349**
**On behalf of Plaintiffs and the Class**

106. Plaintiffs incorporate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

107. Plaintiffs bring this claim on behalf of the Class pursuant to the laws of the State of New York.

108. New York General Business Law § 349(a) ("NYGBL § 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in New York State.

109. Plaintiffs and Class members are consumers and/or persons who have been injured as result of Defendants' violations of NYGBL § 349.

110. As one of the largest companies furnishing healthcare insurance, coverage and services in New York State, Defendants have conducted and continue to conduct business, trade, or commerce in New York State.

111. In the conduct of their business, trade and commerce, and in their furnishing of healthcare insurance, coverage and services in New York State, Defendants' actions were directed at consumers.

112. In the conduct of their business, trade and commerce, and in their furnishing of services in this state, Defendants collected and stored Sensitive Information belonging to Plaintiffs and Class members.

113. In the course of Defendants' business selling their healthcare insurance, coverage and/or services, Defendants willfully failed to disclose that their cybersecurity systems were inadequately protected and that their cybersecurity policies and procedures were inadequately implemented. Moreover, Defendants willfully made affirmative representations that customers' Sensitive Information would be safe in Defendants' care. Furthermore, Defendants willfully failed to disclose the Excellus Breach to Plaintiffs and Class members in a timely manner and waited at least four weeks before informing Plaintiffs and Class members that their Sensitive Information had been compromised.

114. Accordingly, Defendants made untrue, deceptive, and misleading representations of material facts and omitted and/or concealed material facts to Plaintiffs and Class members.

115. Defendants violated NYGBL § 349, and continue to violate NYGBL § 349, by engaging in the deceptive, misleading, and unlawful acts and practices described in this Complaint, including:

- falsely representing to Plaintiffs and Class members that their Sensitive Information provided to Defendants would be safe and secure from theft and unauthorized disclosure;
- falsely representing to Plaintiffs and Class members that Defendants maintained policies and practices sufficient to secure and safeguard Plaintiffs and Class members' Sensitive Information;
- failing to take reasonable steps to secure and safeguard Plaintiffs' and Class members' Sensitive Information in order to prevent its disclosure and theft;
- maintaining IT Systems that Defendants knew were vulnerable to a security breach;
- failing to implement cybersecurity measures commensurate with the duties they undertook by soliciting and storing vast quantities of Plaintiffs' and Class members' Sensitive Information;
- failing to implement a process by which Defendants could detect a breach of their IT Systems in a reasonable period of time; and
- failing to notify Plaintiffs and Class members of the Excellus Breach in a timely and adequate manner.

116. The security of Defendants' data systems was a material fact to Plaintiffs and the Class. Had Plaintiffs and Class members known of Defendants' representations and omissions

as described herein, they would not have purchased healthcare coverage or services from Defendants or provided their Sensitive Information to Defendants.

117. Plaintiffs and Class members suffered injury as a direct and proximate result of Defendants' affirmative untrue, deceptive, and misleading statements and practices, as well as Defendants' omissions and failure to disclose material information.

118. Plaintiffs and Class members overpaid for their healthcare insurance, coverage and/or services and did not receive the benefit of their bargain, as a portion of Defendants' premiums were purported to provide cybersecurity protection to Plaintiffs' and Class members' Sensitive Information.

119. Plaintiffs and Class members are entitled to actual damages as a result of Defendants' unlawful conduct in violation of NYGBL § 349.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that this Court enter a judgment against Defendants and in favor of Plaintiffs and the Class, and award the following relief:

a. that this action may proceed as a class action under New York statute CPLR § 901, that Plaintiffs be appointed as the representatives for the proposed Class, and that Plaintiffs' counsel be appointed as counsel for the proposed Class;

b. award compensatory, consequential, and general damages in an amount to be determined at trial;

c. award Plaintiffs and Class members appropriate relief, including actual and applicable punitive damages;

d. award equitable, injunctive, and declaratory relief as may be appropriate, including without limitation credit monitoring services and identity theft

protection for the lifetime of the Affected Individuals, and an injunction ordering Defendants to immediately notify all Affected Individuals of the Excellus Breach;

e. disgorgement and/or restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices, and the imposition of an equitable constructive trust over all such amounts for the benefits of Plaintiffs and Class members;

f. award all costs of prosecuting the litigation, including expert fees;

g. award pre- and post-judgment interest;

h. award attorneys' fees; and

i. grant such additional relief as this Court may deem just and proper.



**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a trial by jury.

Dated: October 19, 2015

Respectfully submitted,

Matthew J. Fusco
New York Bar No. 2097046
**TREVETT CRISTO**
**SALZER & ANDOLINA, P.C.**
2 State Street, Suite 1000
Rochester, NY 14614
Telephone: (585) 454-2181
Email: mfusco@trevettcristo.com

**KESSLER TOPAZ**
**MELTZER & CHECK, LLP**
Joseph H. Meltzer
New York Bar No. 5065974
Email: jmeltzer@ktmc.com

Naumon A. Amjed (to be admitted *pro hac vice*)
Email: namjed@ktmc.com

Melissa L. Troutner
New York Bar No. 4178208
Email: mtroutner@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

*Attorneys for Plaintiffs Raymond A. McLeod, Juanita McLeod, and the proposed Class*